PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32

A1

(11) International Publication Number: WO 97/50207

(43) International Publication Date: 31 December 1997 (31.12.97)

(21) International Application Number: PCT/SE97/00849

(22) International Filing Date: 23 May 1997 (23.05.97)

(30) Priority Data:
9602528-3 26 June 1996 (26.06.96) SE

(71) Applicant: TELIA AB (publ) [SE/SE]; Mårbackagatan 11, S-123 86 Farsta (SE).

(72) Inventors: LILJEQVIST, Per; Rottnevägen 22, S-128 48 Bagarmossen (SE). CARLSSON, Tommy; Eksätravägen 108, S-756 55 Uppsala (SE). FUCHS, Robert; Timjansgatan 31, S-754 47 Uppsala (SE).

(74) Agent: KARLSSON, Berne; Telia Research AB, Rudsjöterrassen 2, S-136 80 Haninge (SE).

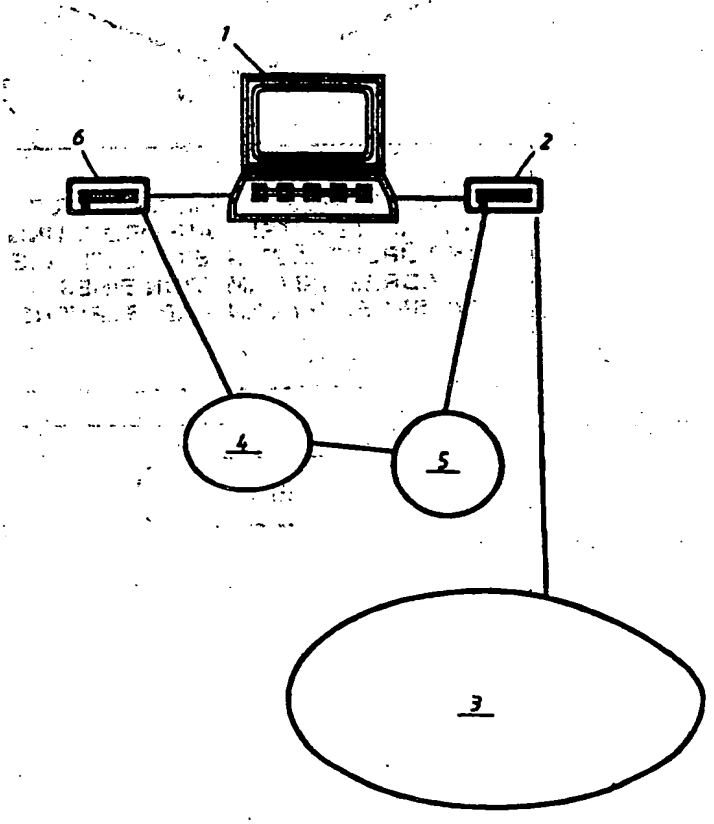
(81) Designated States: NO, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: IMPROVEMENTS IN, OR RELATING TO, INTERNET COMMUNICATION SYSTEMS

(57) Abstract

The invention provides an Internet communication system including a computer terminal, for each Internet-client, and a number of Internet WWW-servers adapted to be accessed by an Internet-client, said computer terminals being adapted for connection to the Internet and having a WWW-browser and a data modem for respectively accessing, and interfacing with, the WWW-servers, characterised in that the communication system includes security means, for said computer terminals and Internet-servers, to ensure that transactions between a WWW-server and an Internet-client are secure. The security means including an Internet-client server for each computer terminal and means for endorsing each transactions with an electronic signature. The Internet-client server has WWW-functionalities and is adapted to link with the data modem and the transaction endorsement means. The security means may be adapted to encrypt and decrypt the transactions. The transaction endorsement means preferably includes a personalised smart card for each Internet-client. The smart card may be used to effect encryption and decryption, as well as providing an electronic signature for the transactions.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

IMPROVEMENTS IN, OR RELATING TO, INTERNET COMMUNICATION SYSTEMS

The invention relates to an Internet communication system, a secure computer terminal, an Internet WWW (World Wide Web)-server for said system, and a method for the secure transmission of information data between an Internet WWW-server and a computer terminal.

The nature, and implementation, of Internet technologies is well known to persons skilled in the art and, whilst the Internet can be attributed with a number of different qualities, security is not one of these attributes. As a consequence of this, use of the public network, provided by the Internet, is excluded for a wide range of applications, for example, business transactions, where security of information is of prime importance.

There is, therefore, a requirement to be able to maintain security of the data traffic as it traverses those sections of the network to which the public has access.

The Internet is, in essence, a global network of interconnected computer terminals, or networks, and comprises a number of separate interconnected networks which are owned and controlled by a number of organisations, for example, network operators, Internet service providers, businesses and universities. The World Wide Web (WWW), known as the 'Web', provides a relatively simple means of accessing, and navigating through the information data provided by Web sites and, in particular, WWW-servers, i.e. computers. WWW-servers can, in effect, be accessed by computer terminal users having the necessary authority from Web site operators, to obtain information data, on any desired topic, stored by the servers. WWW-servers respond to requests for information data, by sending out 'pages' of text, pictures and other information. The information data, comprising a 'page', are combined and displayed on the screen of a user's computer terminal. Web browsers are used to allow access to information held on the Web site servers. In fact, Web-browser

software sends out the requests for 'pages' to Web-servers. The universal language of the Internet is HyperTextMarkup Language (HTML) which is a page description language used on WWW. The storage of information data on a Web site server, i.e. as as 'pages', is effected using HTML and Web site templates.

It is an object of the present invention to provide an Internet communication system for effecting secure transmission of information data between an Internet WWW-server and a computer terminal.

It is another object of the present invention to provide a secure computer terminal for use by Internet-clients.

It is another object of the present invention to provide a secure Internet WWW-server for use by Internet-clients.

It is a further object of the present invention to provide a method for the secure transmission of information data between an Internet WWW-server and a computer terminal.

The present invention provides an Internet communication system including a computer terminal, for each Internet-client, and a number of Internet WWW-servers adapted to be accessed by an Internet-client, said computer terminals being adapted for connection to the Internet and having a WWW-browser and a data modem for respectively accessing, and interfacing with, the WWW-servers, characterised in that the communication system includes security means, for said computer terminals and Internet-servers, to ensure that transactions between a WWW-server and an Internet-client are secure, said security means including an Internet-client server for each computer terminal and means for endorsing each transactions with an electronic signature, and in that said Internet-client server has WWW-functionalities and is adapted to link with said data modem and said transaction endorsement means. The security means may be adapted to encrypt and decrypt said transactions.

The transaction endorsement means may include a personalised smart card for each Internet client, in which case the computer terminals will each include a smart card reader connected to a communication port of a respective computer terminal. The encryption and decryption may be effected by the smart cards.

On the server side of the system, the security means may be arranged behind each of said Internet WWW-servers and adapted to verify said electronic signature. The Internet WWW-server security means are adapted to encrypt and decrypt information. The security means may be arranged behind each of said Internet WWW-servers and use cgi-script and WWW-compatible software.

The system of the present invention may include, for each Internet WWW-server, a storage system for storing verified secure transactions, each of said storage systems being connected to a respective Internet WWW-server. The system may also include a router for each Internet WWW-server, said router being adapted to connect a respective Internet WWW-server to the Internet.

The security means may embody conventional WWW-technology, the use of such technology making the security function transparent.

The system may include means for saving said electronic signature for subsequent use.

The present invention further provides a secure computer terminal for an Internet-client, said terminal being adapted for connection to the Internet and having a WWW-browser and a data modem for respectively accessing, and interfacing with, WWW-servers on the Internet, characterised in that said computer terminal includes security means for ensuring that transactions conducted with a WWW-server are secure, said security means including an Internet-client server and means for endorsing each transaction with an electronic signature, and in that said Internet-client server has WWW-functionalities and is adapted to link with said data modem

and said transaction endorsement means.

The security means may be adapted to encrypt and decrypt said transactions and the transaction endorsement means may include a personalised smart card for a user of said terminal. With this arrangement, the terminal will include a smart card reader connected to a communication port of the computer terminal. The encryption and decryption may be effected by the smart card.

The security means may embody conventional WWW-technology, the use of such technology making the security function transparent.

The present invention further provides a secure Internet WWW-server, said server being adapted to communicate with a secure computer terminal as outlined in preceding paragraphs, characterised in that said Internet WWW-server includes server security means to ensure that transactions conducted with said computer terminal are secure, and in that said server security means are arranged behind said Internet WWW-server and adapted to verify said electronic signature. The server security means which may be adapted to encrypt and decrypt information and which may be arranged behind said WWW-servers as cgi-script and WWW-compatible software, may embody conventional WWW-technology. The use of conventional WWW-technology makes the server security function transparent.

The present invention further provides, in an Internet communication system including a computer terminal, for each Internet-client, and a number of Internet WWW-servers adapted to be accessed by an Internet-client, said computer terminals being adapted for connection to the Internet and having a WWW-browser and a data modem for respectively accessing, and interfacing with, the WWW-servers, a method for the secure transmission of information data between said Internet WWW-server and said computer terminals, characterised by the steps of:

- storing said information data on an intermediate Internet-client server, local to

said computer terminal and having WWW-functionalities;

- endorsing said information data with an electronic signature;
- transmitting the endorsed information data to said Internet WWW-server; and
- on receipt of said endorsed information data by said Internet WWW-server, verifying the electronic signature.

The method may include the steps of:

- encrypting said endorsed information data prior to transmission to said Internet WWW-server; and
- on receipt of said encrypted information data by said Internet WWW-server, decrypting the information date.

The method may also include the steps of:

- encrypting information data prior to transmission from an Internet WWW-server to a computer terminal; and
- on receipt of encrypted information data by said computer terminal, decrypting the information data.

The method may include the step of storing said electronic signature for subsequent identification of the originator of a transaction.

The method step of endorsing said information data with an electronic signature may be effected using a personalised smart card and the personalised smart card may be used to encrypt and decrypt information data.

The information data may be in page-form, the language of said page-form data may be HTML and the page may comprise either separately, or in any combination, text, graphics, pictures, photographs, and fields for entry of information.

Furthermore, the page may be linked to other pages on the same, or other, Internet WWW-servers.

When the page is a form having fields for entry of information, the method may include the steps of obtained said form from an Internet WWW-server; completing said form by entering information in said fields; transferring said completed form to said local intermediate server; endorsing said completed form with an electronic signature; transmitting the endorsed form from said local intermediate server to said Internet WWW-server; and, on receipt of said endorsed form by said Internet WWW-server, verifying the electronic signature. The endorsed form may be encrypted prior to transmission to said Internet WWW-server.

The form may be obtained from an Internet WWW-server, www.xxx.se, and may, for example, contains the following text:

```
<form method = "post" action = "http://localhost/cgi-win/a_script">
<input type = "hidden" name = "data" value = "<data to be signed>">
<input type = "hidden" name = "url" value ="http://www.xxx.se/cgi bin/any_script">
<input type = "submit" value = "Sign"> </form>
```

and method may, in these circumstances, includes the steps of producing an electronic signature on said form, an "a_script" on said local intermediate server being used to effect the signing function; and returning said form to said Internet WWW-server, said form containing, inter alia:

```
<form method = "post" action = "http:/www.xxx.se/cgi-bin/any_script"> <input type = "hidden"
name = "data" value = "<data which has been signed>">
<input type = "hidden" name = "signinfo" value =" <the electronic signature of the data>">
```

<input type = "submit" value = "Transmit"> </form>.

The present invention further provides a communication system operating in accordance with a method, as claimed outlined in preceding paragraphs, for the secure transmission of information data between an Internet WWW-server and an Internet-client.

The present invention further provides an Internet communication system including a secure computer terminal, as outlined in preceding paragraphs, for each Internet-client, and a plurality of Internet WWW-servers, as outlined in preceding paragraphs.

The foregoing and other features according to the present invention will be better understood from the following description, with reference to the accompanying drawings, in which:

Figure 1 diagrammatically illustrates part of an Internet communication system, according to the present invention, including a secure computer terminal for use by Internet-clients.

Figure 2 diagrammatically illustrates another part of an Internet communication system, according to the present invention, including a secure Internet WWW-server for use by Internet-clients.

It will be seen from the following description that an Internet communication system, according to the present invention, provides a more secure arrangement for transactions between an Internet WWW-server and an Internet-client, i.e. the system will facilitate the transmission of information data throughout the essentially public network of the Internet, without the information data being manipulated.

Known Internet communication networks include, in essence, a computer

terminal, for each Internet-client, and a number of Internet WWW-servers adapted to be accessed by an Internet-client. The computer terminals are adapted for connection to the Internet, i.e. have the necessary software and authority for access to the Internet WWW-servers, and having a WWW-browser and a data modem for respectively accessing, and interfacing with, the WWW-servers.

In accordance with the present invention, such a system also includes security means, for the computer terminals and Internet-servers, which are adapted to ensure that transactions between a WWW-server and an Internet-client are secure.

As can be seen from Figure 1 of the accompanying drawings, a secure computer terminal, according to the present invention, includes a computer terminal 1, for example, a personal computer, having a modem 2 for connecting the computer terminal 1 to a public telephone line and thence to the Internet 3, a security module 4, including an Internet-client server 5, for the computer terminal 1, a unit 6, for example, a smart card reader, to provide the means for endorsing each transaction with an electronic signature.

The Internet-client server 5 has WWW-functionalities and is adapted to link with the data modem 2 and the unit 6.

The data modem 2 may, in practice, be integral with, or external to, the computer terminal 1, and is adapted to send and receive information data for a range of applications, including facsimile and e-mail. In any event, the data modem 2 is connected to a communications port of the computer terminal 1.

The required software for the facsimile and e-mail functions is stored on the computer terminal 1 and includes a conventional WWW-browser for obtaining access to the Internet.

Since the Internet is a public network, there is clearly a requirement to be able to effect transactions via the Internet in a secure manner, i.e. the transmission and

receipt of confidential information data via the modem 2. In accordance with the present invention, this is preferably achieved by the use of a personal smart card which holds the personal and security data of the card-holder and allows him, or her, to be identified. Thus, the use of a smart card, in association with a smart card reader 6, will enable each transaction to be signed, electronically, and, where necessary, encrypted in a manner whereby the transaction can be forwarded through different networks without risk of manipulation by third parties. In order to be able to identify, at a later date, the identity of the person who initiated the transaction, the electronic signature may be saved and recovered as, and when, required.

The security function of the present invention can, therefore, be effected through use of a conventional WWW-browser, together with functions for, inter alia, encryption and the handling of smart cards.

The smart card may use asymmetric coding, including public cypher encryption, for effecting the electronic signature and, where necessary, encoding and decoding.

Thus, in accordance with the present invention, secure transactions can be effected on the Internet using the security module 4 and associated WWW-server 5. The module 4 and WWW-server 5 are, therefore, installed on the computer terminal 1 for performing the security functions referred to above. The WWW-server, forming part of the security module 4, is an extremely small WWW-server, of conventional type, which has the functionality to sign, encrypt and decrypt information data. Communication with the smart card reader 6 is handled by the security functions of the module 4 and, to facilitate this, the smart card reader 4 is connected to a communications port of the computer terminal 1.

The security module 4 uses conventional WWW-technology and, as a consequence of this, the security-application becomes transparent (i.e. because WWW-technology is used for both the security module and the remainder of the

system) and can be generalised to match many different services.

It will be seen from Figure 2 of the accompanying drawings that, on the server side of the present invention, a security module 7 is arranged behind a WWW-server 8, and uses cgi-script and conventional software programs, as is normally the case in connection with the WWW. This security module is responsible for:

- verification of electronic signatures;
- encryption of information; and
- decryption of information.

As shown in Figure 2, the WWW-server 8 is connected to the Internet 3, via a router 9, and can, for example, in the case of a bank, be connected to a back-end system 10 to which accepted transactions would be transmitted and stored.

In essence, the WWW will function, under normal circumstances, in the following manner:

- a WWW-client, for example, Netscape, contacts (as a result of an action, for instance a click with an electronic mouse, by a user of the computer terminal 1) a WWW-server, somewhere in the world, and requests the return of a certain 'page', stored on the WWW-server, the requested 'page' may consist of text, graphics, pictures, photographs, and fields for entry of information, etc., but also of links to 'pages' on the same and/or other Web site servers - there may, in fact, be many 'pages' that bring together links to all Web-site relating to a particular topic; and
- when the 'page' consists of a number of fields for entry of information, i.e. the page is a form requiring completion by a recipient, the request, referred to in

(a) above, from the client consists of the completed form; this form is treated on the server-side and, as a result, a new page is returned.

In accordance with the present invention, use is made of conventional WWW-mechanisms, for example, a form is obtained from an external server but, instead of transmitting the completed form directly back to the external server, the form makes an 'intermediate landing' on the WWW-server of the local computer terminal 1, i.e the server 5. The server 5 attends to the signing, and possibly also encryption, of the information, in a manner as outlined above, and, on completion of this process, the form, or 'page', is returned to the WWW-client. The form will not be transmitted to the external server until the user requests such transmission.

As stated above, data which is to be made available on the Internet must be transferred and, if necessary, translated into HTML documents, i.e the universal language of the Internet.

The method used for writing on a HTML-page is outlined below, in relation to the:

- recovery of information data from a 'page', or more particularly, from a WWW-form; and
- application of an electronic signature to the information data to facilitate the secure transmission of the information data through the various public networks.

In accordance with the present invention, a small local WWW-server 5 is installed on the computer terminal 1 and the conventional WWW-procedures for handling forms are then used, in a manner known to persons skilled in the art, to effect the process. In other words, in accordance with normal procedures for forms, a cgi-script is called on the local server with data to which an electronic signature is

to be applied, i.e. from the server www.xxx.se comes (as a result of a previous form) a 'page' which contains, for example:

```
<form method = "post" action = "http://localhost/cgi-win/a_script">
<input type = "hidden" name = "data" value = "<data to be signed>">
<input type = "hidden" name = "url" value ="http://www.xxx.se/cgi bin/any_script">
<input type = "submit" value = "Sign"> </form>,
```

"a_script" on the local server (local host) making use of the signing function to produce an electronic signature to the data and then returns a page which, among other things, contains:

```
<form method = "post" action = "http:/www.xxx.se/cgi-bin/any_script"> <input type = "hidden"
name ="data" value ="<data which has been signed>">
<input type = "hidden" name = "signinfo" value =" <the electronic signature of the data>">
<input type = "submit" value = "Transmit"> </form>
```

Since the security function of the present invention is based on conventional WWW-technology, it is independent of which browser is used and which server is used, i.e. no interference is necessary either in a browser, or in a server, in respect of which the security function is used. In addition, the security function of the present invention is relatively easy to adapt to different levels of security and to new technologies. This makes the present invention very flexible and cost effective in that it can be readily adapted to meet specific security requirements which may be demanded by a user and/or service provider.

It will be directly evident from the foregoing that the present invention can be used in many applications, where security of information is of prime importance, for example, to:

- perform business transactions, such as, bank transactions, or the purchase of goods;

- indicate authority for performing actions, such as, logging on to a system, or obtaining access to certain information;

- encrypt information which shall be transmitted over the WWW; and

- decrypt information which has been published encrypted on the WWW.

In addition, the use of the security function of the present invention gives rise to the following advantages:

- use of conventional WWW-technologies; this means that services which are developed on this medium are placed on the server-side and become accessible to everybody without any distribution problems - all logic in the service itself is on the server-side;

- no dependence on which browser, or server, is used;

- no interference necessary with either the browser, or the server;

- relatively inexpensive; and

- flexible, in that it can be adapted to meet different levels of security, the use of a smart card representing the highest level of security.

The solution to the Internet security problems, presented by the present invention, can be effected using all Windows-platforms; (3.x, Win95, NT). However, the invention could be adapted for use on other platforms, such as, UNIX, or the Macintosh-platform, by suitably adjusting the porting arrangements.

CLAIMS

1. An Internet communication system including a computer terminal, for each Internet-client, and a number of Internet WWW-servers adapted to be accessed by an Internet-client, said computer terminals being adapted for connection to the Internet and having a WWW-browser and a data modem for respectively accessing, and interfacing with, the WWW-servers, characterised in that the communication system includes security means, for said computer terminals and Internet-servers, to ensure that transactions between a WWW-server and an Internet-client are secure, said security means including an Internet-client server for each computer terminal and means for endorsing each transactions with an electronic signature, and in that said Internet-client server has WWW-functionalities and is adapted to link with said data modem and said transaction endorsement means.

2. A system as claimed in claim 1, characterised in that said security means are adapted to encrypt and decrypt said transactions.

3. A system as claimed in claim 1, or claim 2, characterised in that said transaction endorsement means includes a personalised smart card for each Internet client, and in that said computer terminals each include a smart card reader connected to a communication port of a respective computer terminal.

4. A system as claimed in claim 3, when appended to claim 2, characterised in that said encryption and decryption is effected by said smart cards.

5. A system as claimed in any one of the preceding claims, characterised in that said security means are arranged behind each of said Internet WWW-servers and are adapted to verify said electronic signature.

6. A system as claimed in claim 5, characterised in that said Internet WWW-server security means are adapted to encrypt and decrypt information.

7. A system as claimed in claim 5, or claim 6, characterised in that said security means are arranged behind each of said Internet WWW-servers and uses cgi-script and WWW-compatible software.

8. A system as claimed in any of claims 5 to 7, characterised in that said system includes, for each Internet WWW-server, a storage system for storing verified secure transactions, each of said storage systems being connected to a respective Internet WWW-server.

9. A system as claimed in any of claims 5 to 8, characterised in that said system includes a router for each Internet WWW-server, said router being adapted to connect a respective Internet WWW-server to the Internet.

10. A system as claimed in any one of the preceding claims, characterised in that said security means embody conventional WWW-technology.

11. A system as claimed in claim 10, characterised in that use of conventional WWW-technology makes the security function transparent.

12. A system as claimed in any one of the preceding claims, characterised in that said system includes means for saving said electronic signature for subsequent use.

13. A secure computer terminal for an Internet-client, said terminal being adapted for connection to the Internet and having a WWW-browser and a data modem for respectively accessing, and interfacing with, WWW-servers on the Internet, characterised in that said computer terminal includes security means for ensuring that transactions conducted with a WWW-server are secure, said security means including an Internet-client server and means for endorsing each transaction with an electronic signature, and in that said Internet-client server has WWW-functionalities and is adapted to link with said data modem and said transaction endorsement means.

14. A terminal as claimed in claim 13, characterised in that said security means are adapted to encrypt and decrypt said transactions.

15. A terminal as claimed in claim 13, or claim 14, characterised in that said transaction endorsement means includes a personalised smart card for a user of said terminal, and in that said terminal includes a smart card reader, said reader being connected to a communication port of said terminal.

16. A terminal as claimed in claim 15, when appended to claim 14, characterised in that said encryption and decryption is effected by said smart card.

17. A terminal as claimed in any one of claims 13 to 16, characterised in that said security means embody conventional WWW-technology.

18. A terminal as claimed in claim 17, characterised in that use of conventional WWW-technology makes the security function transparent.

19. A secure Internet WWW-server, said server being adapted to communicate with a secure computer terminal as claimed in any one of the claims 13 to 18, characterised in that said Internet WWW-server includes server security means to ensure that transactions conducted with said computer terminal are secure, and in that said server security means are arranged behind said Internet WWW-server and adapted to verify said electronic signature.

20. A WWW-server as claimed in claim 19, characterised in that said server security means are adapted to encrypt and decrypt information.

21. A WWW-server as claimed in claim 19, or claim 20, characterised in that said server security means are arranged behind said WWW-servers as cgi-script and WWW-compatible software.

22. A WWW-server as claimed in any one of claims 19 to 21, characterised in that said server security means embody conventional WWW-technology.

23. A WWW-server as claimed in claim 22, characterised in that use of conventional WWW-technology makes the server security function transparent.

24. In an Internet communication system including a computer terminal, for each Internet-client, and a number of Internet WWW-servers adapted to be accessed by an Internet-client, said computer terminals being adapted for connection to the Internet and having a WWW-browser and a data modem for respectively accessing, and interfacing with, the WWW-servers, a method for the secure transmission of information data between said Internet WWW-server and said computer terminals, characterised by the steps of:

- storing said information data on an intermediate Internet-client server, local to said computer terminal and having WWW-functionalities;
- endorsing said information data with an electronic signature;
- transmitting the endorsed information data to said Internet WWW-server; and
- on receipt of said endorsed information data by said Internet WWW-server, verifying the electronic signature.

25. A method as claimed in claim 24, characterised by the steps of:

- encrypting said endorsed information data prior to transmission to said Internet WWW-server; and
- on receipt of said encrypted information data by said Internet WWW-server, decrypting the information date.

26. A method as claimed in claim 24, or claim 25, characterised by the steps of:

- encrypting information data prior to transmission from an Internet WWW-server to a computer terminal; and

- on receipt of encrypted information data by said computer terminal, decrypting the information data.

27. A method as claimed in any one of the claims 24 to 26, characterised by the step of storing said electronic signature for subsequent identification of the originator of a transaction.

28. A method as claimed in any one of claims 24 to 27, characterised in that the step of endorsing said information data with an electronic signature is effected using a personalised smart card.

29. A method as claimed in claim 28, characterised in that said personalised smart card is used to encrypt and decrypt information data.

30. A method as claimed in any one of the claims 24 to 29, characterised in that said information data is in page-form, the language of said page-form data being HTML.

31. A method as claimed in claim 30, characterised in that said page consist of any one, or more, of the following:

- text;

- graphics;

- pictures;

- photographs; and

- fields for entry of information.

32. A method as claimed in claim 30, characterised in that said page is linked to other pages on the same, or other, Internet WWW-servers.

33. A method as claimed in claim 31, characterised in that said page is a form having fields for entry of information, and in that the method includes the steps of:

- obtained said form from an Internet WWW-server;

- completing said form by entering information in said fields;

- transferring said completed form to said local intermediate server;

- endorsing said completed form with an electronic signature;

- transmitting the endorsed form from said local intermediate server to said Internet WWW-server; and

- on receipt of said endorsed form by said Internet WWW-server, verifying the electronic signature.

34. A method as claimed in claim 33, characterised in that said endorsed form is encrypted prior to transmission to said Internet WWW-server.

35. A method as claimed in claim 33, or claim 34, characterised in that said form is obtained from an Internet WWW-server, www.xxx.se, and contains the following text:

<form method = "post" action = "http://localhost/cgi-win/a_script">
<input type = "hidden" name = "data" value = "<data to be signed>">
<input type = "hidden" name = "url" value ="http://www.xxx.se/cgi bin/any_script">
<input type = "submit" value = "Sign"> </form>

and in that said method includes the steps of:

- producing an electronic signature on said form, an "a_script" on said local intermediate server being used to effect the signing function; and

- returning said form to said Internet WWW-server, said form containing, inter alia:

<form method = "post" action = "http:/www.xxx.se/cgi-bin/any_script"> <input type = "hidden" name = "data" value = "<data which has been signed>">
<input type = "hidden" name = "signinfo" value =" <the electronic signature of the data>">
<input type = "submit" value = "Transmit"> </form>

36. A communication system operating in accordance with a method, as claimed in any one of the claims 24 to 35, for the secure transmission of information data between an Internet WWW-server and an Internet-client.

37. An Internet communication system including a secure computer terminal, as claimed in any of claims 13 to 18, for each Internet-client, and a plurality of Internet WWW-servers, as claimed in any of claims 19 to 23.

Fig. 1

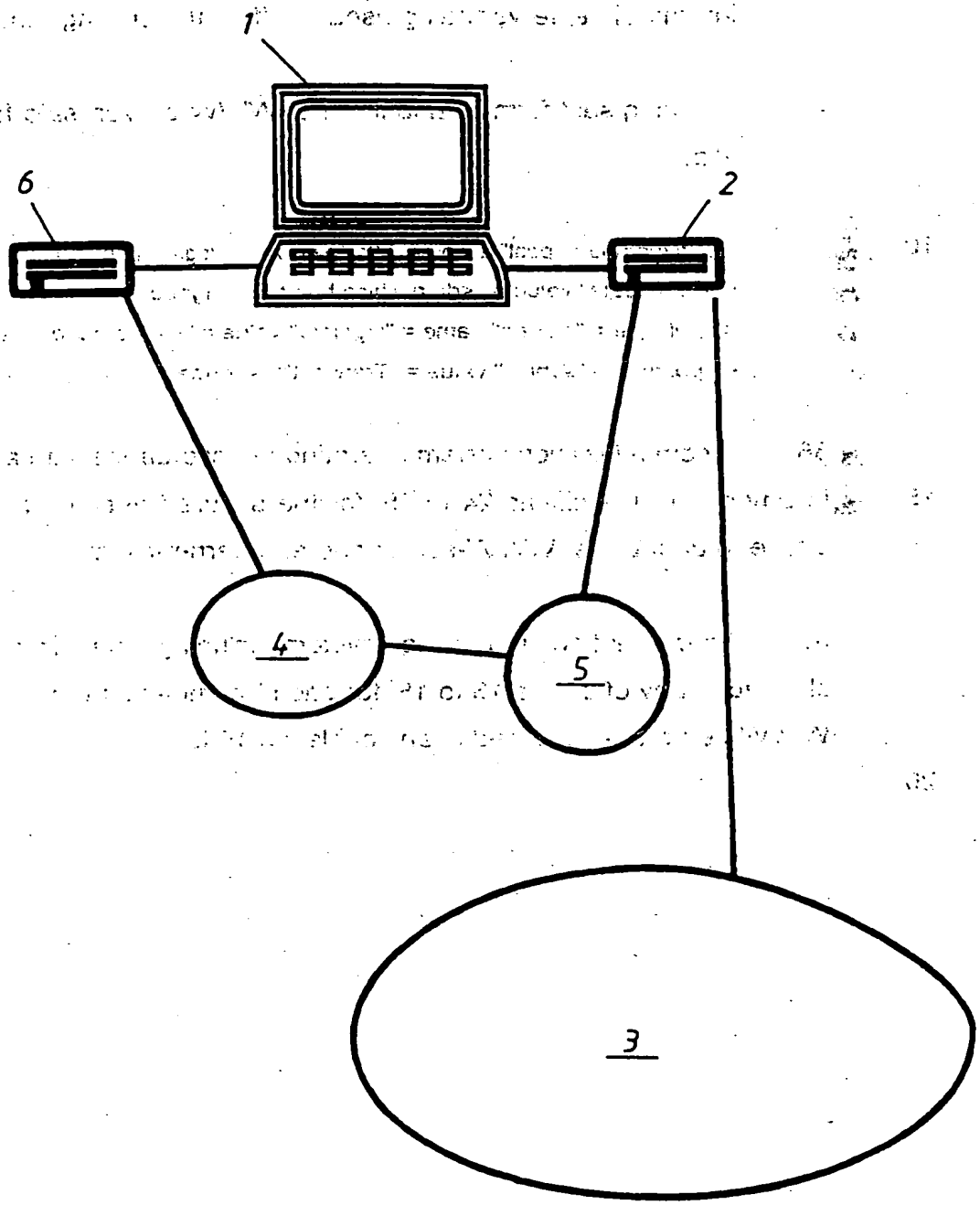
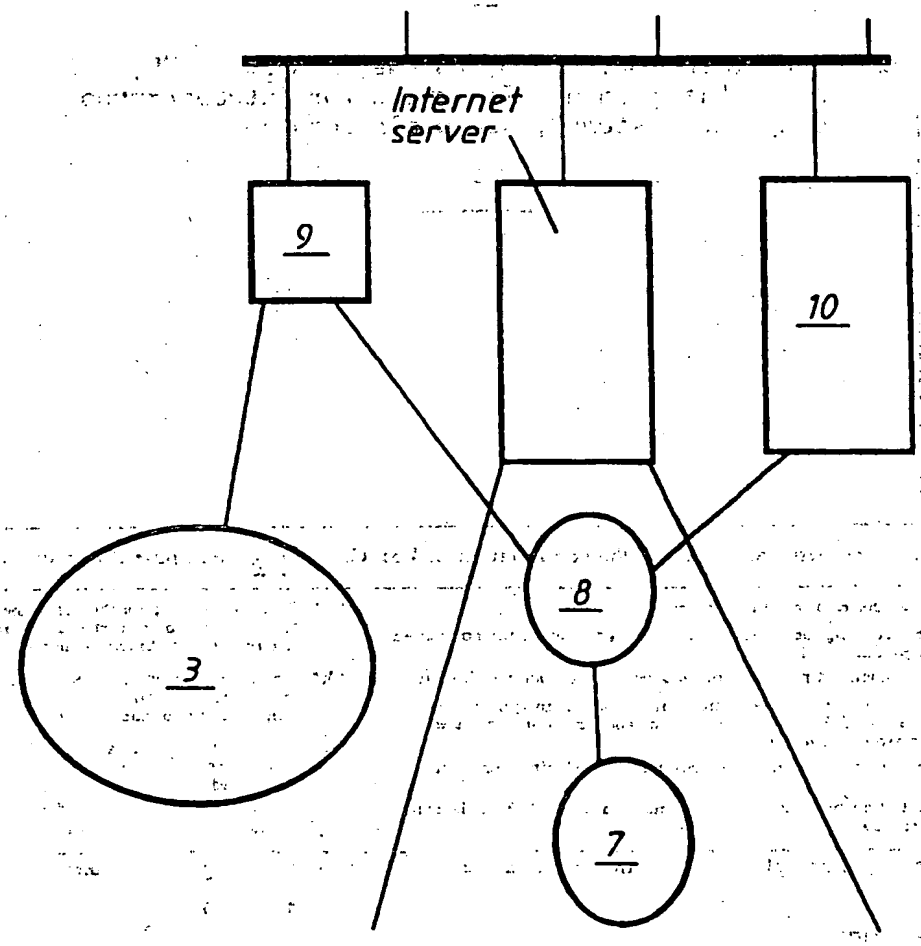


Fig. 2



INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 97/00849

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5475757 A (JOSEPH P. KELLY), 12 December 1995 (12.12.95), figure 1, abstract ---	1-37
Y	IEEE Spectrum, pp: 22-26, Volume, August 1989, Karen Fitzgerald, "The quest for intruder-proof computer systems", see whole document --- ---	1-37

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" erlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 Sept 1997	23-09-1997
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

01/09/97

International application No.
PCT/SE 97/00849

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5475757 A	12/12/95	EP 0687087 A	13/12/95
		JP 8023330 A	23/01/96